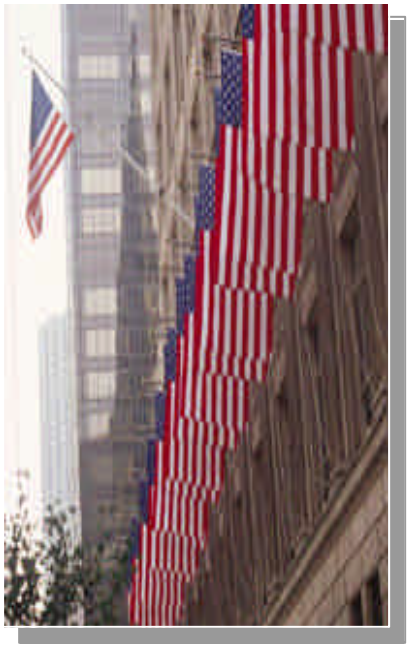
Oracle Corporation



Jack Pellicci
Group Vice President
Oracle Government, Education and Health

Building Trust and Protecting Privacy

Digital Government Boot Camp 2002

October 8, 2002

ORACLE

Building Trust and Protecting Privacy

- What is the Impact of Government Transformation?
  - Convergence of e-Gov and Homeland Security
  - Meeting Privacy and Security Requirements in a World of Online Government
- What is the Relationship Between Security and Privacy?
- What do Citizens/ Businesses want?
- What is the Role of Government vs. Industry?
- How can government build trust?
- What Best Practices Can Help in Building a Privacy Program in Government?
- Do We Need Consistent Policies at Federal and State/ Local Levels?
- What are Some Basic Guidelines for Government to Follow ?

Transforming the Government Enterprise

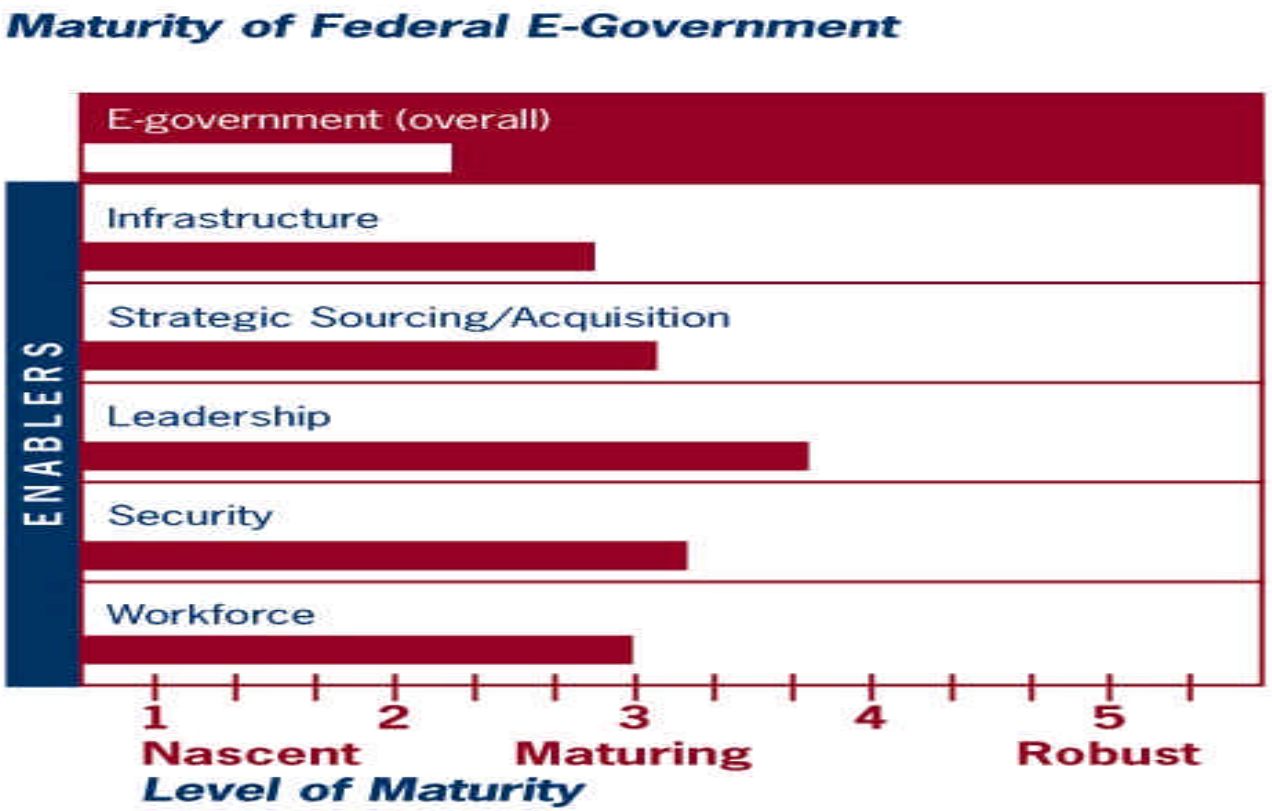
- Service to → Service by
- In Line → On-Line
- e-Commerce → e-Business
- Physical Knowledge → Digital Knowledge
- Casual Security → Acute Security
- Information Sharing → Assured Privacy

Focus on Core Values to Maintain Trust and Confidence

On Line Government and Privacy

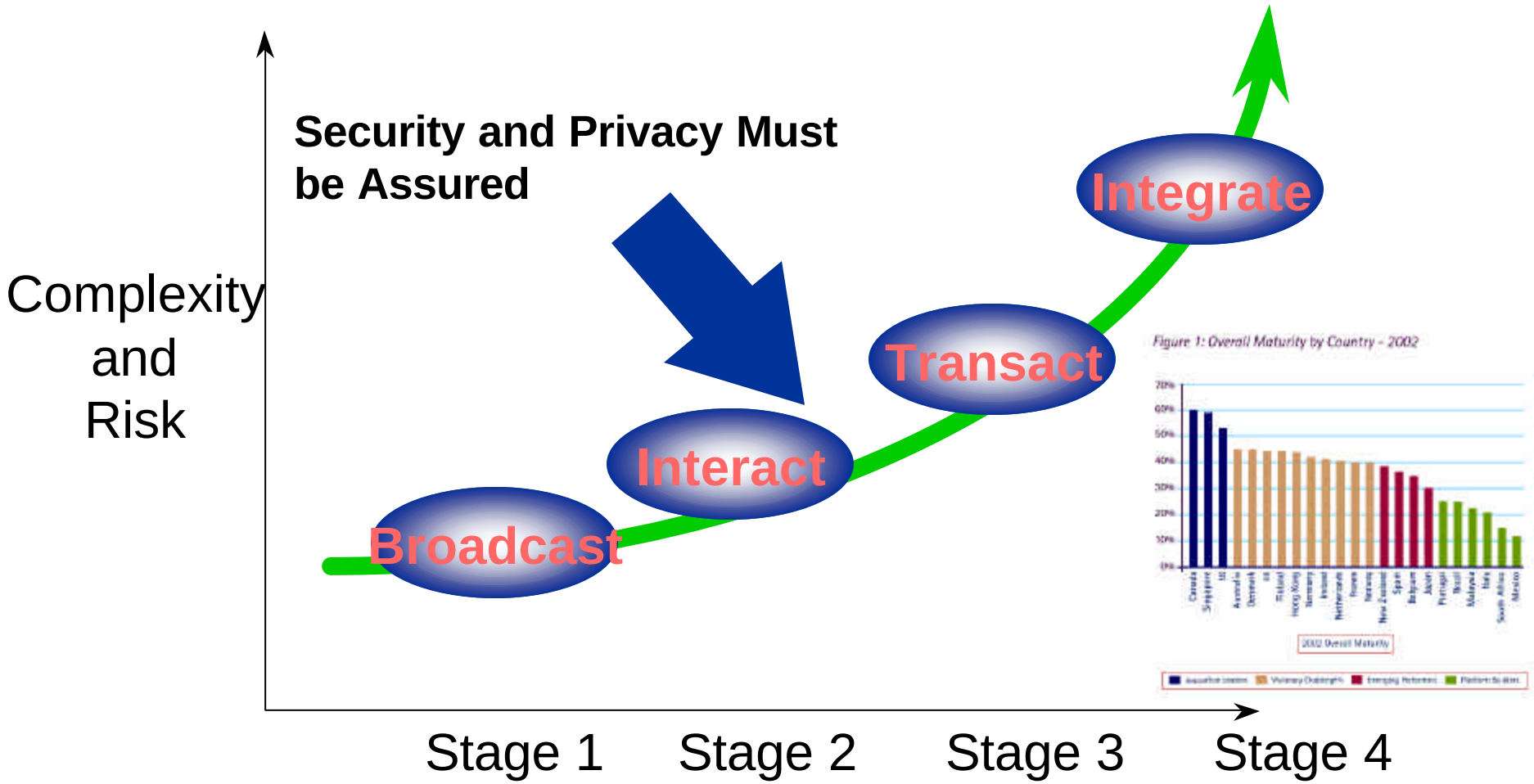
Government to Government	Government to Citizen/Business	Government to Supplier/Partner	Government to Employee

Security and Privacy Levels in Federal



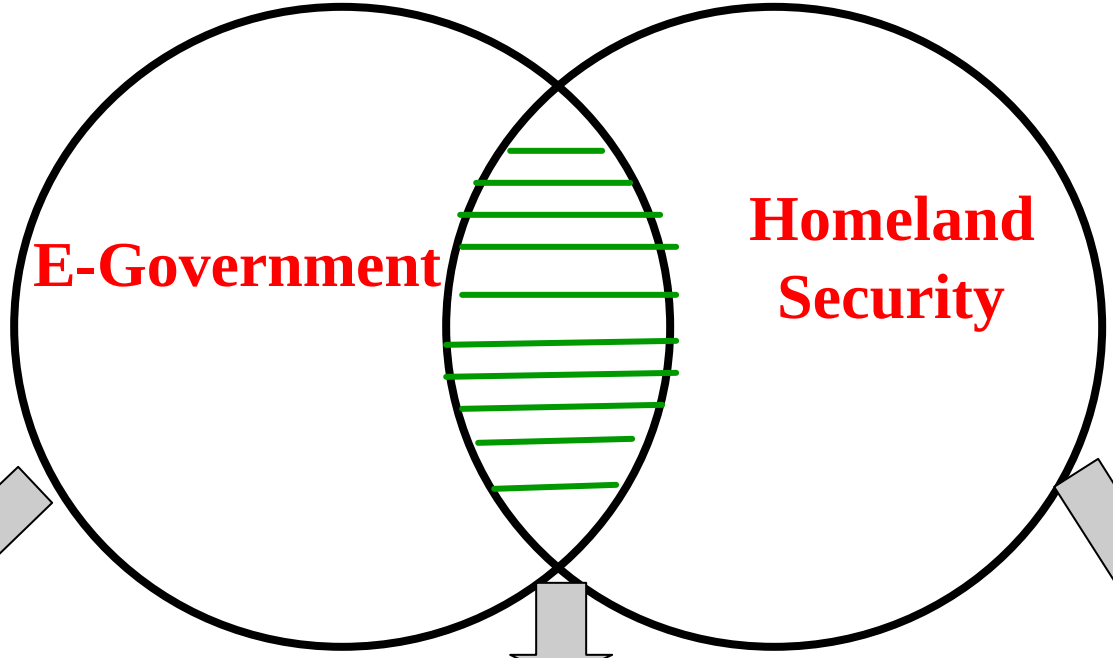
E-Government

Each stage increases risk to security and privacy



Impact of E-Government and Homeland Security Convergence

Digital Government with a National Purpose



- Effectiveness
- Efficiency
- Service Delivery

Balancing Requirements

- Security
- Privacy
- Trust
- Confidence
- Operational Excellence

- Prevent Attacks
- Reduce Vulnerability
- Recover Quickly

Building Trust and Protecting Privacy

- Major Concerns
  - Unauthorized Access
  - Identity Theft
  - Credit Card Theft
  - Online Fraud
  - Hacker Intrusions
  - Viruses
  - Terrorism

The threat: Computer Security Institute and FBI survey

- 90% detected security breaches
- 60% external, 40% internal
- 71% detected unauthorized access by insiders
- Average loss per intrusion:
  - External : $57,000
  - Internal: $2,700,000

The Internet provides much greater access to data, and to more valuable data, not only to legitimate users, but also hackers, disgruntled employees, criminals, and corporate spies

ORACLE

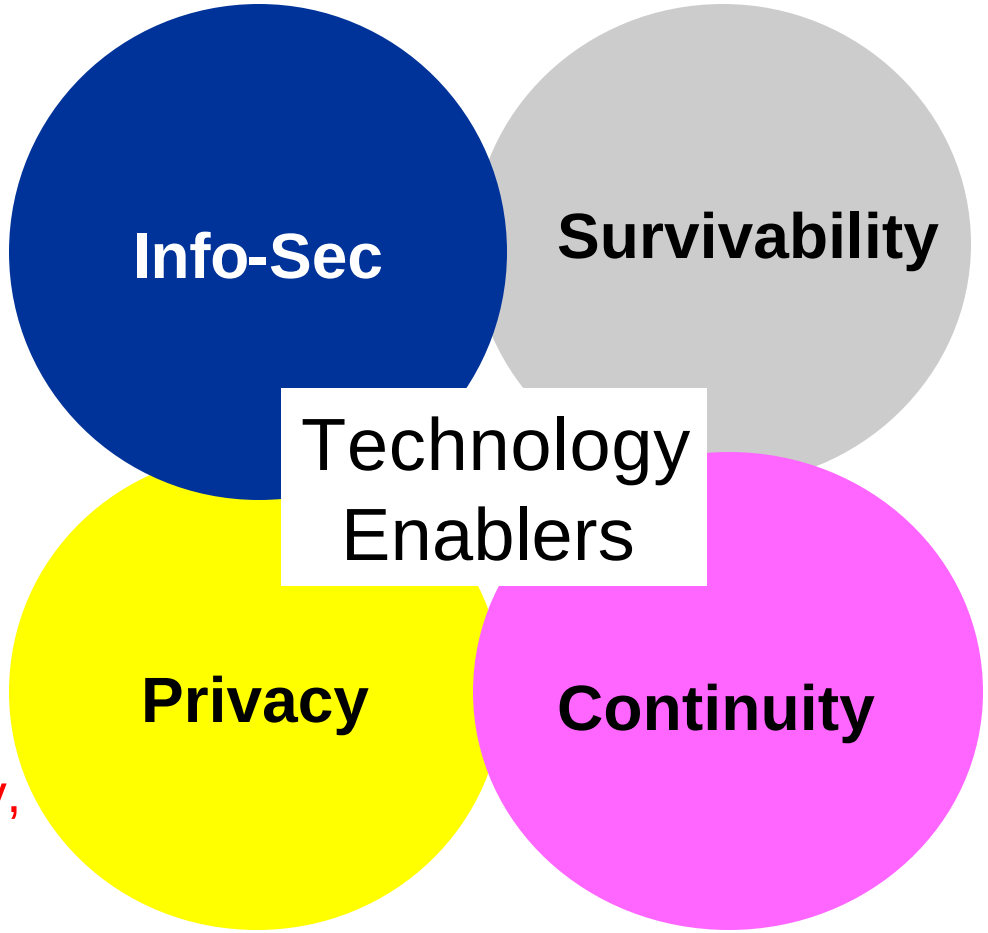
Source: Computer Security Institute and FBI Survey

Citizens and Consumers Are Concerned

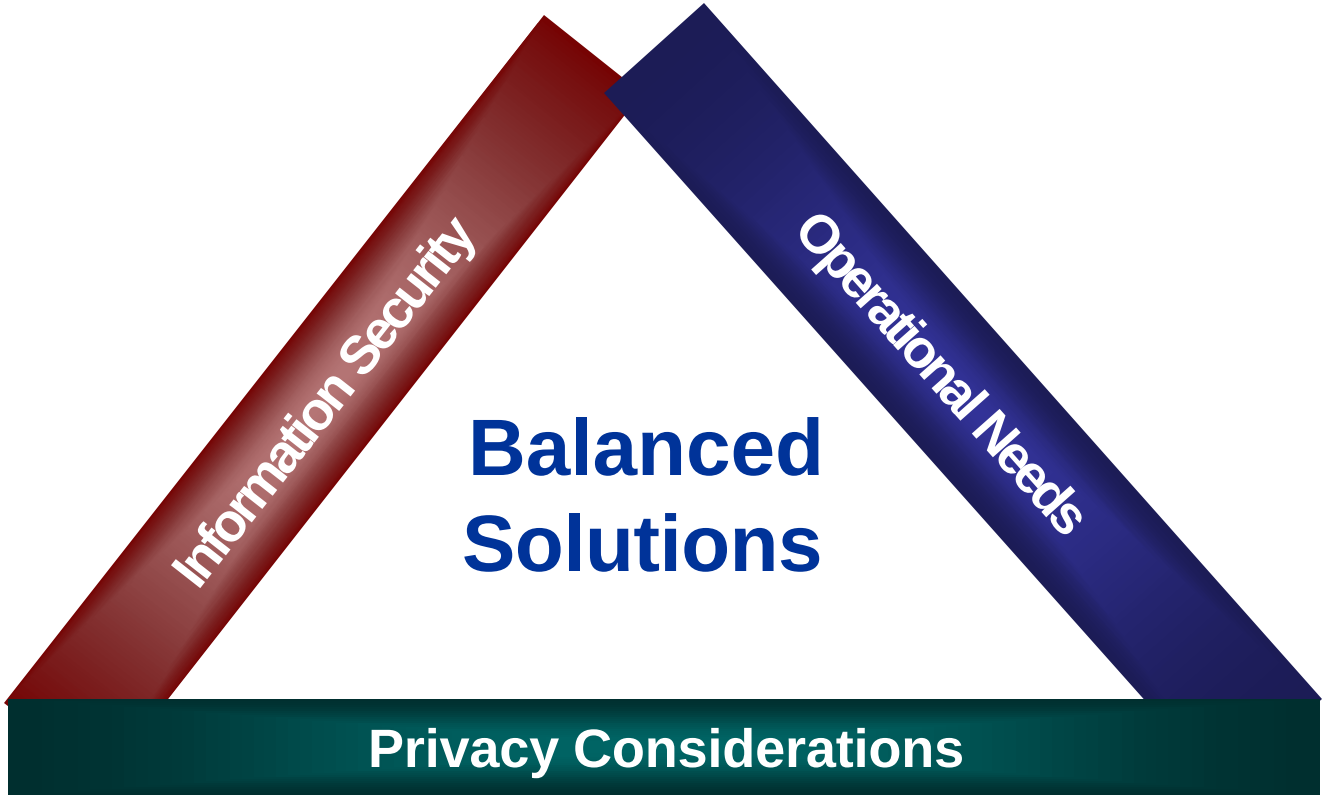
- ITAA survey, December 2001:
  - 70% of Americans concerned about Internet and computer security
  - 74% expressed fears that their personal information on the Internet could be stolen or used for malicious purposes.
  - 74% number said they are concerned that cyber-attacks could target critical infrastructure assets like telephone networks or power plants.
- Improved security will build trust

Putting Privacy in Perspective

- Information Security
  -- Secure, Protect, Defend
- Survivability
- Continuity of Operations
- Privacy
  -- Policy Driven Protection of Personal Information
- Technology
  -- Enables Info-Sec, Survivability, Continuity and Privacy



Balancing the Approach



Considerations for Balancing Security With Privacy

- Operational Requirements
  - Efficiency
  - Productivity
  - Cost
- Choice
  - Personal Security
  - Personal Privacy
- Risk
  - Making the tradeoff when required

Good Security Enhances Privacy

- Multilevel Security
- International Security evaluations
- Common Criteria/ ISO
- Virtual Private Database
- Label Security
- Fine-grained auditing
- Data Encryption (DES, 3DES, RC4-256)
- Password Maintenance
- Multi-tier Authentication

Build Trust by Strengthening Security

Decreasing the Risk

- Building Online Trust Means Creating Better Information Security
  - Make InfoSec First Tier Priority
  - Appropriate Sufficient Funds Strengthen Basic Infrastructure
  - Coordinate Policies Across Fed/ S/L Governments
  - Reach Out to International Counterparts
  - Share Best Practices/Encourage Better Practices
  - Focus on People and Processes, not Just Technology (e.g. Insider Threat)

Government Actions

- **What Can Government Do?**
  - Fund Information Security efforts
    - FY 03 Budget requests should be fully authorized
    - 15.5% increase in overall government IT budget
    - 64% increase in information security spending
    - Industry pushing aggressively
    - Increase state level funding of computer crime units

Government Actions.. Continued

- **Act as Issue Champion**
  - Promote Private Sector Action
    - Cyber Corps – Resources and Training
    - SME Awareness
  - Advance Research and Development—especially Research
  - Create Grants to State and Local Governments, University Programs
  - Continue Funding Increases for Cyber Corps
  - Promote Privacy Audits
  - Require Privacy Impact Statements

Private Sector Approach

- Industry Moving Rapidly to Address Security and Privacy Issues:
  - Security and Privacy Balanced based on Operational Requirements
  - Privacy Policy Notification Widespread
  - Consumer Control Over Personal Data
  - Automation of Privacy Preferences
  - Privacy Seal Programs

Summary: Basic Privacy Guidelines for Consideration

- Focus on Core Values That Build Trust
- Enact Policies That Have High Probability of Working and Are minimally Intrusive
- Announce and Explain New Security Procedures That Might Impinge on Privacy
- Measure the Effects of Enacted Policies
- Leverage Technology to Provide Security and Support Privacy Without Undermining Trust

Long Term Solutions for Measurable Results